(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開平11－66008
(43)公開日　平成11年(1999)３月９日

| (51)Int.Cl.* | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| Ｇ０６Ｆ | 15/00 | ３３０ | Ｇ０６Ｆ | 15/00 | ３３０Ｇ |
| Ａ６３Ｆ | 9/22 | | Ａ６３Ｆ | 9/22 | Ｇ |
| Ｇ０６Ｆ | 12/14 | ３２０ | Ｇ０６Ｆ | 12/14 | ３２０Ｆ |
| | 17/60 | | | 15/21 | ３４０Ｂ |
| Ｇ０７Ｆ | 7/12 | | Ｇ０７Ｆ | 7/08 | Ｂ |

審査請求　未請求　請求項の数９　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平9－231107

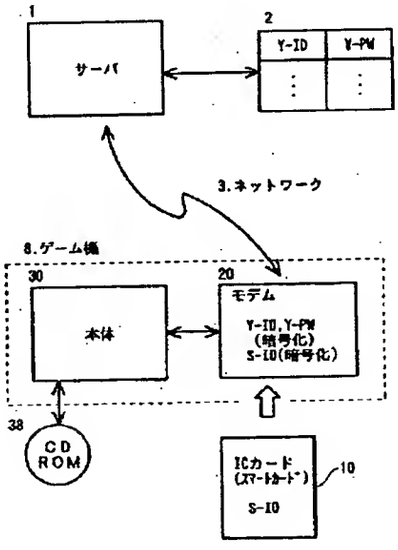
(22)出願日　平成９年(1997)８月27日

(71)出願人　000132471
株式会社セガ・エンタープライゼス
東京都大田区羽田１丁目２番12号
(72)発明者　川堀　昌樹
東京都大田区羽田１丁目２番12号　株式会社セガ・エンタープライゼス内
(74)代理人　弁理士　土井　健二　（外１名）

(54)【発明の名称】　ＩＣカードを利用したゲーム装置

(57)【要約】
【課題】認証情報である英数字をアクセスのたびに入力する煩雑さを解消する。
【解決手段】本発明は、モデム装置が装着可能であって、モデム装置を装着してからサーバに通信回線を介して接続され、認証情報を送信してサーバで正規ユーザである認証を受けた時に、一定のサービスを受けることができるゲーム装置において、正規ユーザに与えられるＩＣカードのカードＩＤと認証情報とが記録される記録媒体がモデム装置に設けられ、モデム装置に挿入されたＩＣカードのカードＩＤが、記録媒体に記録されたカードＩＤと一致する時に、記録された前記認証情報が前記サーバに送信されることを特徴とする。ＩＣカードのカードＩＤを鍵データにして、記録媒体への認証用情報の記録に鍵をかけることにより、不正使用に対する耐性を高くし、アクセスするたびに認証用の英数字を入力する煩雑さを解消することができる。

第一の実施の形態例の概略図



1

【特許請求の範囲】
【請求項１】サーバに通信回線を介して接続され、認証情報を送信してサーバで正規ユーザである認証を受けた時に、一定のサービスを受けることができる通信端末装置において、
前記正規ユーザに与えられるＩＣカードのカードＩＤを鍵データにして、前記認証情報が記録される記録媒体を有し、
挿入されたＩＣカードのカードＩＤを鍵データにして、前記記録媒体に記録された前記認証情報が前記サーバに送信されることを特徴とする通信端末装置。
【請求項２】サーバに通信回線を介して接続され、認証情報を送信してサーバで正規ユーザである認証を受けた時に、一定のサービスを受けることができる通信端末装置において、
前記正規ユーザに与えられるＩＣカードのカードＩＤと前記認証情報とが記録される記録媒体を有し、
前記挿入されたＩＣカードのカードＩＤが、前記記録媒体に記録されたカードＩＤと一致する時に、前記記録された前記認証情報が前記サーバに送信されることを特徴とする通信端末装置。
【請求項３】モデム装置が装着可能であって、該モデム装置を装着してからサーバに通信回線を介して接続され、認証情報を送信してサーバで正規ユーザである認証を受けた時に、一定のサービスを受けることができるゲーム装置において、
前記正規ユーザに与えられるＩＣカードのカードＩＤと前記認証情報とが記録される記録媒体が前記モデム装置に設けられ、
前記モデム装置に挿入されたＩＣカードのカードＩＤが、前記記録媒体に記録されたカードＩＤと一致する時に、前記記録された前記認証情報が前記サーバに送信されることを特徴とするゲーム装置。
【請求項４】請求項３において、
前記記録媒体への認証情報の記録または消去が、前記ＩＣカードが挿入されたことを条件に可能であることを特徴とするゲーム装置。
【請求項５】サーバに通信回線を介して接続され、使用許諾を要求するプログラムデータを送信し、前記サーバから使用許諾パスワードを受信し、所定のプログラムの使用を前記使用許諾パスワードによって使用可能にする通信端末装置において、
前記通信端末装置に挿入されたＩＣカードのカードＩＤを前記サーバに送信可能であり、
前記サーバにて前記カードＩＤを鍵データにして暗号化された前記使用許諾パスワードが記録される記録媒体を有し、
挿入された前記ＩＣカードのカードＩＤを鍵データにして前記記録媒体に記録された暗号化使用許諾パスワードが復号化されることを特徴とする通信端末装置。

2

【請求項６】請求項５において、
前記記録媒体は、前記カードＩＤも使用許諾パスワードと共に記録可能であり、前記挿入された前記ＩＣカードのカードＩＤが前記記録されたカードＩＤと一致する時に、前記復号化が許可されることを特徴とする通信端末装置。
【請求項７】サーバと通信端末装置とが通信回線を介して接続可能に構成され、前記通信端末装置における所定のプログラムの使用を許可する使用許諾パスワードの管理方法において、
（ａ）前記通信端末装置に挿入されたＩＣカードのカードＩＤと共に前記プログラムのＩＤを、前記通信端末装置から前記サーバに送信する工程と、
（ｂ）前記サーバは、前記送信されたプログラムＩＤに対応する使用許諾パスワードを前記送信されたカードＩＤを鍵データとして暗号化し、該暗号化された使用許諾パスワードを前記通信端末装置に送信する工程と、
（ｃ）前記通信端末装置は、前記送信された暗号化された使用許諾パスワードを記録媒体に記録する工程と、
（ｄ）前記通信端末装置に挿入されたＩＣカードに記録されたカードＩＤを鍵データにして、前記記録された暗号化使用許諾パスワードを復号化し、該復号化された使用許諾パスワードを使用して前記プログラムの使用をする工程とを有することを特徴とするプログラムの使用許諾パスワードの管理方法。
【請求項８】請求項７において、
更に、（ｅ）前記サーバは、前記カードＩＤと送信した使用許諾パスワードとの対応テーブルを記録する工程と、
（ｆ）前記通信端末装置から前記カードＩＤが送られた時、前記対応テーブルに記録された該カードＩＤに対応する使用許諾パスワードを前記カードＩＤにより暗号化して送信する工程とを有することを特徴とする使用許諾パスワードの管理方法。
【請求項９】請求項７において、
更に、（ｇ）前記サーバは、前記工程（ｂ）において前記暗号化された使用許諾パスワードを前記通信端末装置に送信する時に、前記ＩＣカードに記録されているクレジット度数を減少する工程と、
（ｈ）前記サーバは、前記カードＩＤに対応する最新のクレジット度数データを保管する工程と、
前記工程（ａ）において、前記通信端末装置は、挿入されたＩＣカードのクレジット度数データも併せて前記サーバに送信し、
前記工程（ｂ）において、前記サーバは、受信したクレジット度数データと前記保管された最新のクレジット度数データとを照合し、一致する場合に前記使用許諾パスワードを暗号化して送信することを特徴とする使用許諾パスワードの管理方法。
【発明の詳細な説明】

【０００１】
【発明の属する技術分野】本発明は、ネットワークを介してセンタのサーバにアクセスする為のユーザのＩＤやパスワード等の個人認証のための情報を記録して、容易に送信可能にするとともに、その記録した個人認証の情報のセキュリティを高くすることができるゲーム装置または端末装置に関する。
【０００２】
【従来の技術】送信機能を有するゲーム装置や端末装置をネットワークを介してセンタのサーバに正規ユーザであるか否かを認証する為の情報として、ユーザＩＤとそれに対するユーザパスワード等が送信される。そして、サーバ側では、予め登録されているユーザＩＤとユーザパスワードの照合を取り、正規ユーザか否かの認証を行う。
【０００３】一般には、このユーザＩＤやユーザパスワードは、無意味な英数字の文字列であり、これらの文字列をネットワークのサーバに接続するたびにユーザがゲーム装置や端末装置から入力することは煩雑である。特に、ゲーム機の場合は、通常入力用のキーボードを有しておらず、接続したテレビ画面上に表示されたソフトウエアキーボードにより入力する必要があり、その場合は、英数字の入力は益々煩雑である。
【０００４】また、ユーザの認証用の情報だけでなく、ゲームのプログラムを格納した記録媒体を流通させ、それぞれのゲームプログラムの各ステージ毎にパスワードを課金するたびにネットワークを通じてユーザに与えるゲームプログラムの超流通においても、ゲーム・パスワードを入力する必要がある。その場合も、そのゲーム・パスワードを毎回入力する作業はユーザにとって煩雑である。
【０００５】
【発明が解決しようとする課題】上記のサーバに接続するたびに認証用の情報を入力したり、ゲームプログラムを実行するたびにゲーム・パスワードを入力する作業を省略する為に、それらの情報をゲーム機や端末装置内の不揮発性のメモリに記録する方法が考えられる。
【０００６】しかしながら、単純にゲーム機や端末装置の不揮発性メモリに情報を記録すると、容易にコピーされ、それらの情報が正規ユーザからの情報であるか否かの個人認証のセキュリティが低くなることが問題となる。即ち、ゲーム機や端末装置の不揮発性メモリに情報を記録する方法では、ユーザがゲーム機や端末装置を所有していることを根拠にして認証を行うことになる。その為に、ゲーム機や端末装置の不正使用者に対して耐性の低いシステムとなる。また、多数のユーザがゲーム機や端末装置を共有するシステムにおいては、上記の方法では、ユーザの認証が適切に行われない。
【０００７】そこで、本発明の目的は、通信機能を有するゲーム機や通信端末装置において、認証用の情報やパスワードをセキュリティが高く、不正使用に対して耐性が高く記録されるゲーム機または通信端末装置を提供することにある。



【０００８】
【課題を解決するための手段】上記の目的を達成する為に、本発明は、サーバに通信回線を介して接続され、認証情報を送信してサーバで正規ユーザである認証を受けた時に、一定のサービスを受けることができる通信端末装置において、前記正規ユーザに与えられるＩＣカードのカードＩＤを鍵データにして、前記認証情報が記録される記録媒体を有し、挿入されたＩＣカードのカードＩＤを鍵データにして、前記記録媒体に記録された前記認証情報が前記サーバに送信されることを特徴とする。
【０００９】ＩＣカードのカードＩＤを鍵データにして、記録媒体への認証用情報の記録に鍵をかけることにより、不正使用に対する耐性を高くし、アクセスするたびに認証用の英数字を入力する煩雑さを解消することができる。
【００１０】また、上記の目的を達成する為に、本発明は、サーバと通信端末装置とが通信回線を介して接続可能に構成され、前記通信端末装置における所定のプログラムの使用を許可する使用許諾パスワードの管理方法において、（ａ）前記通信端末装置に挿入されたＩＣカードのカードＩＤと共に前記プログラムのＩＤを、前記通信端末装置から前記サーバに送信する工程と、（ｂ）前記サーバは、前記送信されたプログラムＩＤに対応する使用許諾パスワードを前記送信されたカードＩＤを鍵データとして暗号化し、該暗号化された使用許諾パスワードを前記通信端末装置に送信する工程と、（ｃ）前記通信端末装置は、前記送信された暗号化された使用許諾パスワードを記録媒体に記録する工程と、（ｄ）前記通信端末装置に挿入されたＩＣカードに記録されたカードＩＤを鍵データにして、前記記録された暗号化使用許諾パスワードを復号化し、該復号化された使用許諾パスワードを使用して前記プログラムの使用をする工程とを有することを特徴とする。
【００１１】ＩＣカードのカードＩＤを鍵データに利用してプログラムの使用許諾パスワードを暗号化して通信端末装置のメモリに記録するので、使用許諾パスワードそのものをユーザに開示することなく、そのサービスを提供することができる。また、記録しておくことで、プログラムを使用するたびに使用許諾パスワードを入力する煩雑さは解消される。しかも、ＩＣカードと通信端末装置の記録媒体とを物理的に分離することで、不正使用に対する耐性を高くすることができる。
【００１２】
【発明の実施の形態】以下、本発明の実施の形態について図面に従って説明する。しかしながら、本発明の技術的範囲がその実施の形態に限定されるものではない。
【００１３】［第一の実施の形態例（個人認証の情

報）］図１は、第一の実施の形態例の全体構成を示す図である。第一の実施の形態例では、個人認証用の情報をゲーム機や通信端末装置の不揮発性メモリに記録し、且つ、一般に複製が困難なＩＣカード（別名スマートカード）に記録されているＩＣカードに固有の情報を鍵データにして、その記録に電子的な鍵をかける。

【００１４】図１に示される通り、サーバ１に電話回線等のネットワーク３を介してゲーム機６が接続される。本発明はゲーム機だけでなく通信端末装置から認証情報を送信する場合にも適用できるが、ここではゲーム機を例にして説明する。図１の例では、ゲーム機６の本体３０には通信機能がないので、それに接続されるモデム２０を介してサーバ１と接続される。但し、モデム２０が本体３０と一体化されてゲーム機６が構成されても良い。そして、ゲーム機６内のモデム２０内の不揮発性メモリ内に、認証用の情報であるユーザＩＤとそれに対するユーザパスワードとが記録される。このモデム２０内の不揮発性メモリ内の情報は、一般に読み出しが困難な状態にある。

【００１５】更に、重要なことは、正規ユーザのみが所有するＩＣカード１０のユニークなＩＤ（スマートカードのＩＤとして以下Ｓ－ＩＤ）を鍵にして、モデム２０内の不揮発性メモリ内に記録された認証用情報の記録に電子的な鍵がかけられる点にある。即ち、モデム２０内の不揮発性メモリ内に、ユーザＩＤ：Ｙ－ＩＤ、ユーザパスワードＹ－ＰＷに加えて、ＩＣカードのＩＤとしてＳ－ＩＤを記録する。そして、ゲーム機６に正規ユーザが所有するＩＣカードが装着されて、そのカードのＩＤであるＳ－ＩＤとモデム２０内の不揮発性メモリに記録されているカードＩＤ：Ｓ－ＩＤとが一致する場合のみ、個人認証用のユーザＩＤ：Ｙ－ＩＤとユーザ・パスワードＹ－ＰＷとがネットワークを通じてサーバ１に送信される様にする。

【００１６】ここで、ＩＣカード１０は、例えばネットワークを介してゲーム機６をサーバ１に接続し、ゲームプログラムの使用のサービスを受けたり、別途流通させたゲームプログラムを格納した記録媒体３８の使用許諾パスワードを受信するサービスを受ける時の、課金に利用される。即ち、予めサービスを利用する為の料金の支払いを条件にＩＣカードがプリペードカードとして正規のユーザに譲渡される。従って、本実施の形態例ではその正規ユーザが所有するＩＣカード内のユニークな情報であるカードＩＤ：Ｓ－ＩＤを、電子的な鍵データとして利用する。

【００１７】この方式によれば、ＩＣカードを所有する正規ユーザが、同様に正規ユーザが所有するゲーム機６を使用する場合のみ、不揮発性メモリ内に記録された認証用の情報であるユーザＩＤ：Ｙ－ＩＤとユーザパスワードＹ－ＰＷとがサーバ１に送信されるので、非常にセキュリティが高く、不正使用者に対する耐性が高いシステムとなる。認証用情報とＩＣカードＩＤ：Ｓ－ＩＤとは、モデム２０内の不揮発性メモリでなく、ゲーム機の本体３０内のメモリに記録される場合でも良いが、それらの情報の複製を困難にするためには、モデム２０内の不揮発性メモリに記録するのが適切である。



【００１８】更に、この方式によれば、正規ユーザが第三者にＩＣカードとゲーム機６またはモデム２０を貸与することにより、第三者に認証用の情報を開示することなく、ネットワークを通じての所定のサービスを第三者に受けることを許可することができる。従って、店頭などで不特定多数のユーザに対して、ネットワークを介してサーバ１に接続したデモを提供することが可能になる。

【００１９】また、モデム２０内の不揮発性メモリに認証用情報やＩＣカードＩＤを記録する場合、ゲームプログラムが格納された記録媒体３８内に格納されているゲームプログラムに共通する鍵データを利用して、認証用情報Ｙ－ＩＤ，Ｙ－ＰＷやＩＣカードＩＤ：Ｓ－ＩＤを暗号化して記録することもできる。

【００２０】尚、サーバ１側では、ユーザＩＤ：Ｙ－ＩＤとユーザ・パスワードＹ－ＰＷとの照合を行う為のテーブルがファイル装置２に記録される。サーバ１では、送信されるユーザＩＤ：Ｙ－ＩＤとユーザ・パスワードＹ－ＰＷとの照合を上記ファイル装置２内のテーブルを参照することで行い、正規ユーザか否かの認証を行う。

【００２１】図２は、ゲーム機とＩＤカードの詳細構成を示す図である。この例では、テレビ等のモニタ画面４０に接続されるゲーム本体３０に、通信機能を付加する為のモデム装置２０がモデムスロット３１に挿入可能になっている。更に、そのモデム装置２０にプリペードカードなどに利用されるＩＣカード１０がカードスロット２１に挿入可能になっている。

【００２２】ＩＣカード１０には、課金情報としてクレジットデータ（度数）が格納されサービスを受けるたびに課金の為のクレジットデータを減少する処理が行われる不揮発性メモリ領域１１と、ＩＣカードのシリアル番号などのカードにユニークなＩＤ：Ｓ－ＩＤが記録されたリードオンリーメモリ（ＲＯＭ）１２とが少なくとも備えられている。

【００２３】モデム２０には、カードスロット２１と、モデム機能を有するモデムチップ２２と不揮発性メモリ２５とがバス２６を介して接続される。また、モデムチップ２２は、接続端子２３を介して電話線などの通信回線２４に接続される。

【００２４】ゲーム機の本体３０には、外部の入力操作装置３９との接続を行うＩ／Ｏ部３６、外部のテレビモニタ４０に画像データを供給するビデオプロセッサ３５、外部のゲームプログラムを格納したＣＤＲＯＭやゲームカートリッジなどの記録媒体３８からプログラムやデータを読み出す装置３７、バックアップ用メモリ３

４、そして、ゲームプログラムや通信プログラムを実行するＣＰＵ３２、そしてＲＡＭ３３が、バス４１を介して接続される。

【００２５】ゲーム機の本体３０のモデムスロット３１にモデム装置２０を装着することで、通信機能付きのゲーム装置となる。そして、必要に応じて、ＩＣカード１０がモデム装置２０のカードスロット２１に装着される。

【００２６】図３は、ゲーム機のモデム２０内の不揮発性メモリ２５内に情報が保存され、それが使用される場合のフローチャートを示す図である。認証用のユーザＩＤ：Ｙ－ＩＤとユーザパスワードＹ－ＰＷ及びカードＩＤ：Ｓ－ＩＤとがモデム２０内のメモリ２５に保存される場合や、それらの情報がモデム２０内のメモリ２５から消去される場合には、少なくともＩＣカード１０がカードスロット２１に装着されることが必要条件である。そうすることにより、店頭などでゲーム機６をサーバ１に接続してのデモを不特定多数の顧客に提供する場合でも、顧客によってそれらの情報が不正に消去されたり書き換えられたりすることを防止する。

【００２７】図３に従ってフローチャートを説明する。このフローチャートに示される処理フローは、外部の記録媒体３８内に格納されている通信ソフトウエアに従って、ゲーム機の本体１０とモデム装置２０とにより実現される。

【００２８】まず、ステップＳ１０、Ｓ１２にて、ＩＣカードがモデム装置２０のカードスロット２１に挿入されているか否か、挿入されている場合に、ＩＣカード内のＲＯＭのカードＩＤ：Ｓ－ＩＤとモデム装置２０内の不揮発性メモリ２５に記録されているカードＩＤ：Ｓ－ＩＤとが一致するか否かが判定される。例えば、既にＩＣカード内のカードＩＤ：Ｓ－ＩＤがモデム２０の不揮発性メモリ２５内に記録されている場合は、両カードＩＤ：Ｓ－ＩＤが一致するので、ステップＳ２６にてモデム２０内の不揮発性メモリ２５に記録されているユーザＩＤ：Ｙ－ＩＤとユーザパスワードＹ－ＰＷとが自動的に送信される。従って、毎回ソフトウエアキーボードからそれらの認証情報である英数字列を入力する必要はない。

【００２９】例えば、ＩＣカードが挿入されているが、カードＩＤ：Ｓ－ＩＤが一致しない場合や、ＩＣカードそのものが挿入されていない場合は、モニタ画面４０にユーザＩＤとユーザパスワードとを入力する画面が表示される（ステップＳ１４）。そこで、ユーザがソフトウエアキーボードから認証に必要な情報であるユーザＩＤ：Ｙ－ＩＤとユーザパスワードＹ－ＰＷとをキー入力する（ステップＳ１６）。そこで、ＩＣカードの挿入を要求するメッセージが表示されてから（Ｓ１８）、ＩＣカードが挿入されていて（Ｓ２０）、モデムの不揮発性メモリ２５内に情報（認証情報と鍵データ）が記録されていないまたはその記録されている情報（認証情報と鍵データ）が入力された情報と一致しない場合（Ｓ２２）は、ユーザＩＤ：Ｙ－ＩＤ．ユーザパスワードＹ－ＰＷ．そしてカードＩＤ：Ｓ－ＩＤの保存、または消去が可能になる（Ｓ２４）。

【００３０】上記のフローチャートに従って、以下異なる操作手順について説明する。

【００３１】手順１は、正規ユーザが．初めてＩＣカードをモデム装置に挿入して、認証情報であるユーザＩＤ：Ｙ－ＩＤとユーザパスワードＹ－ＰＷ及びＩＣカードのキー情報であるカードＩＤ：Ｓ－ＩＤを不揮発性メモリ２５に記録する場合である。

【００３２】この場合は、ステップＳ１０，Ｓ１２により、カードＩＤが一致しないと判定され、ステップＳ１４で入力画面が表示され、正規ユーザによりユーザＩＤ：Ｙ－ＩＤとユーザパスワードＹ－ＰＷとが入力される（Ｓ１６）。この場合は、モデムの不揮発性メモリ２５内に認証情報のカードＩＤやユーザＩＤやパスワード及び鍵データ等の情報が未書き込みなため（Ｓ２２）、入力されたユーザＩＤ：Ｙ－ＩＤ、ユーザパスワードＹ－ＰＷ及び、ＩＣカード内に記録されているカードＩＤ：Ｓ－ＩＤ（鍵データ）が、暗号化されて、モデム２０内の不揮発性メモリ２５に保存され（Ｓ２４）、ユーザＩＤ：Ｙ－ＩＤとユーザパスワードＹ－ＰＷとが送信される（Ｓ２６）。上記の暗号化のキーデータは、通信ソフトウエア内に存在する。

【００３３】手順２は、正規ユーザが、上記手順１で登録した後にＩＣカードを挿入して、認証情報の送信を自動で行う場合である。まず、正規ユーザは、正規のＩＣカードを挿入する。ＩＣカード内にＲＯＭに記録されているカードＩＤ：Ｓ－ＩＤが、モデム２０の不揮発性メモリ２５内に記録されているカードＩＤ：Ｓ－ＩＤと一致するので（Ｓ１２）、ステップＳ２６にて、モデムのメモリ２５に記録されているユーザＩＤ：Ｙ－ＩＤとユーザパスワードＹ－ＰＷとが送信される。従って、正規ユーザは、毎回認証情報をキー入力する手間を省くことができる。また、正規ユーザは、友人などに認証情報を開示することなくＩＣカードを貸与してサービスを受けることを可能にすることができる。

【００３４】手順３は、正規ユーザがＩＣカードを挿入せずに使用する場合である。この場合は、ＩＣカードが挿入されていないので、ステップＳ１４で認証情報の入力画面となり（Ｓ１４）、正規ユーザは記憶しているユーザＩＤ：Ｙ－ＩＤとユーザパスワードＹ－ＰＷとを入力する（Ｓ１６）。そして、ＩＣカードが挿入されていないので（Ｓ２０）、ステップＳ２６にて、入力した認証情報が送信される。この場合は、正規ユーザがＩＣカードを利用しない場合の例である。ＩＣカードを挿入しない限り、モデム内のメモリ２５の情報の消去、書換は行われない。

【００３５】手順４は、モデムの不揮発性メモリ２５内に保存データが存在するが、ＩＣカード内のカードＩＤ：Ｓ－ＩＤと一致しない場合である。例えば、正規ユーザが新しいＩＣカードを入手した場合である。この場合は、ＩＣカードが挿入されているが（Ｓ１０）、鍵データであるそのカードＩＤ：Ｓ－ＩＤとモデム内の不揮発性メモリ２５内のカードＩＤ：Ｓ－ＩＤとが不一致のため（Ｓ１２）、認証情報の入力画面になり（Ｓ１４）、ユーザが入力する（Ｓ１６）。そこで、ＩＣカードが挿入されているが（Ｓ２０）、モデムの不揮発性メモリ２５内の情報が不一致であるので、ユーザがステップ２４にてその情報を消去または保存を選択して（Ｓ２４）、入力した認証情報を送信する（Ｓ２６）。

【００３６】手順５は、正規ユーザが認証情報を変更する場合である。従って、既にモデムのメモリ２５には、古い認証情報と鍵データのＩＣカードのカードＩＤ：Ｓ－ＩＤとが記憶されている。この場合は、最初にＩＣカードを挿入しない。その結果、認証情報入力画面となる（Ｓ１４）。そこで、正規ユーザが新たな認証情報を入力すると（Ｓ１６）、ＩＣカードの挿入が促される（Ｓ１８）。そこで、ＩＣカードを挿入すると、入力した認証情報と書き込み済の認証情報とが不一致であるので、ステップＳ２４にてそれらの情報の消去または入力情報の保存を行うことができる。その後、認証情報が送信される（Ｓ２６）。この場合も、ＩＣカードを所有する正規ユーザによってのみ情報の消去や保存が可能になる。

【００３７】手順６は、第三者が不正に取得したＩＣカードを利用してサーバからサービスを受けようとする場合である。この場合は、ＩＣカードのカードＩＤ：Ｓ－ＩＤとモデム内のメモリの鍵データであるカードＩＤ：Ｓ－ＩＤとが不一致となり、自動的に認証情報が送信されることはない。従って、第三者は、正しい認証情報を所有していないので、サーバから認証を受けることはない。

【００３８】手順７は、店頭で不特定多数の顧客にデモを提供する場合である。この場合は、例えばモデムに挿入されるＩＣカードを顧客から隔離しておくことで、顧客は認証情報を知ることなく、デモの提供を受けることができる。

【００３９】図３のフローチャートに示される通り、最初にＩＣカードの挿入の有無と鍵データの一致とがチェックされる。ＩＣカードが挿入され鍵データであるカードＩＤ：Ｓ－ＩＤが一致する場合は、認証情報の自動送信を行うが、それ以外の場合は、認証情報の入力画面に移行する（Ｓ１４）。また、認証情報が入力された後は、ＩＣカードが挿入されていれば（Ｓ２０）、モデムの不揮発性メモリ２５内に書き込まれた情報と入力した情報及び鍵データとが一致しなければ、それらの情報の消去または保存がユーザにより選択される。

【００４０】図４は、第一の実施の形態例の変形例を示す図である。この図は、図１と同じ部分には同じ引用番号を付した。この変形例では、モデム２０の不揮発性メモリ２５に認証情報であるユーザＩＤ：Ｙ－ＩＤとユーザパスワードＹ－ＰＷとを記録する時、挿入されているＩＣカードのカードＩＤ：Ｓ－ＩＤを鍵データにして暗号化されたデータが記録される。従って、正規ユーザまたは正規ユーザから正規に貸与された第三者が正規のＩＣカードを挿入した場合にのみ、ＩＣカード内のカードＩＤ：Ｓ－ＩＤを鍵データにしてモデムの不揮発性メモリに記録された認証情報を復号化して、サーバに送信し、認証を得ることができる。この場合も、サーバに接続する毎に認証情報をキー入力する必要がなく、しかも認証情報はセキュリティの高い方法で記録される。また、第三者に認証情報を開示することなく、ＩＣカードを貸与してサービスの提供を許可することが可能になる。

【００４１】［第二の実施の形態例］第二の実施の形態例は、第一の実施の形態例と同様にＩＣカード（通称スマートカード）にユニークに与えられたカードＩＤ：Ｓ－ＩＤを鍵データとして利用して、経済的価値を有する使用許諾パスワードをゲーム機のメモリに記録することを特徴とする。

【００４２】ゲームプログラムに限らず、一般のプログラムの場合でも、プログラムのサンプルまたは一部の使用を許可したプログラムを格納した記録媒体を無償若しくは廉価で流通させ、ユーザがそれを使用してみて更に全部の機能を利用したい場合に、クレジットカードやプリペードカードなどの形態で料金を支払い、それを条件に使用できるパスワードを提供することが行われる。この方法であれば、ユーザは自らプログラムまたはゲームを試してみて、気に入ったプログラムまたはその一部分にのみ使用料金を支払うことができ、ユーザの利便性を上げよりプログラムの普及を図ることができる。この様な形式において、プログラムやゲームの継続使用できるパスワードは、経済的価値を有し、秘密の状態で使用すべきである。

【００４３】ところが、正規のパスワード所有者は、無意味な英数字の文字列からなるパスワードを毎回入力することは煩雑である。更に、この使用許諾パスワードは、複製されることにより第三者がプログラムを使用することができ、無限の経済的価値を生む可能性がある。そこで、第一の実施の形態例と同様に毎回の入力の煩雑さを避ける為に、ゲーム装置や端末装置内の不揮発性メモリにパスワードをＩＣカードのカードＩＤ：Ｓ－ＩＤを鍵データにして記録して、ＩＣカードを所有する正規のユーザが正規のゲーム機や端末装置にＩＣカードを挿入した場合にのみパスワードの出力が許可される様にする。更に、この使用許諾パスワードを、正規ユーザが所有するＩＣカードのカードＩＤ：Ｓ－ＩＤを鍵データとして暗号化した形態で、ユーザに提供する。こうするこ

とで、パスワード自体のデータをユーザに知らせずにパスワードの持つ価値をユーザに提供することができる。更に、ＩＣカードの所有をこの使用許諾パスワードの利用の条件とすることで、パスワードのコピーによる不正使用を防止することができ、不正な第三者に対するセキュリティを高くすることができる。

【００４４】図５は、第二の実施の形態例の概略図である。この例では、ビデオゲームのプログラムの使用許諾パスワードをゲームパスワードＧ－ＰＷとしてユーザに与える例である。更に、ビデオゲームで、ロールプレイングゲーム等、ゲーム内に複数のステージが存在し、ユーザが最初のステージから開始して、各ステージをクリアするたびに、次のステージの使用を許諾するゲームパスワードＧ－ＰＷが必要になる例である。

【００４５】まず、サーバ１は、その外部記憶ファイル４に、ゲームＩＤ：Ｇ－ＩＤとステージＩＤ：Ｓｔａｇｅ－ＩＤの組み合わせに対するゲームパスワードＧ－ＰＷの対応テーブルを記録する。そして、ユーザは、ゲーム機６を通信回線であるネットワークを介してサーバ１に接続し、取得したいゲームパスワードのゲームＩＤ：Ｇ－ＩＤとステージＩＤ：Ｓｔａｇｅ－１Ｄとを、ＩＣカードのカードＩＤ：Ｓ－ＩＤと共にサーバに送信する。

【００４６】サーバ１側では、対応テーブルからゲームパスワードＧ－ＰＷを検出し、そのゲームパスワードＧ－ＰＷをカードＩＤ：Ｓ－ＩＤを鍵データとして暗号化し、その暗号化されたゲームパスワードＧ－ＰＷを、ネットワークを介してゲーム機６に送信する。それと同時にサーバ側は課金処理を行う。ゲーム機６では、モデム２０内の不揮発性メモリ内に暗号化されたゲームパスワードＧ－ＰＷと、その暗号化の鍵データであるカードＩＤ：Ｓ－ＩＤとを記録する。カードＩＤ：Ｓ－ＩＤの記録は、第一の実施の形態例の如く、通信プログラムに内蔵された暗号化アルゴリズムで暗号化される。

【００４７】その後、ゲーム機６では、ＩＣカードを所有する正規のユーザがＩＣカードをモデム２０に挿入した場合に、ＩＣカード１０のカードＩＤ：Ｓ－ＩＤとモデム２０のメモリに記録されたカードＩＤ：Ｓ－ＩＤとを照合し、一致することを条件として、暗号化されたゲームパスワードＧ－ＰＷをカードＩＤ：Ｓ－ＩＤを鍵データとして復号化し、そのゲームパスワードＧ－ＰＷを使用してゲームプログラムの該当する部分を使用可能にする。

【００４８】上記の第二の実施の形態例では、第一の実施の形態例と同様に、図２に示されたゲーム本体３０、モデム２０及びＩＣカード１０とが使用される。そして、第一の実施の形態例と同様にして、ＩＣカードのカードＩＤ：Ｓ－ＩＤが、ゲームパスワードＧ－ＰＷを読み出す為の鍵データとして使用される。しかも、カードＩＤ：Ｓ－ＩＤを鍵データに利用してゲームパスワードを暗号化しているので、ゲームパスワードのコピーによる不正使用に対する耐性は非常に高い。第一の実施の形態例と同様に、正規ユーザが所有するＩＣカードとゲーム機のモデム２０とが同時に使用されるときのみ．ゲームパスワードの使用が可能になるので、ゲームパスワードの入力作業を省略することができ、しかも、不正使用に対する耐性が高い。

【００４９】第二の実施の形態例の第一の変形例として、ユーザがサーバ１に送るデータとして、ゲームＩＤ：Ｇ－ＩＤとステージＩＤ：Ｓｔａｇｅ－ＩＤとＩＣカードのカードＩＤ：Ｓ－１Ｄに、さらにＩＣカードのメモリ１１に記録されたプリペードデータであるクレジットデータを追加する。サービスの利用料金を予め支払うことで、使用度数を記録したクレジットデータを記録したＩＣカードが提供される。そして、サービスを利用するたびに課金処理として、そのクレジットデータの度数をクレジットダウン（使用度数の減少処理）させることが行われる。即ち、この変形例は、ＩＣカードがプリペードカードとして使用される場合に適用できる。

【００５０】この変形例では、更にサーバ１側で、カードＩＤ：Ｓ－ＩＤと最新のクレジットデータとの対応テーブルを外部ファイル７に記録しておく。そこで、サーバ１側では、ユーザから送信されるカードＩＤ：Ｓ－ＩＤとクレジットデータとを、その外部ファイル７内の対応テーブルを参照することにより、正規ユーザからのアクセスであるか否かをチェックする。

【００５１】このクレジットデータを送信データに追加することで、ネット上を送信されたゲームＩＤ：Ｇ－ＩＤ、ステージＩＤ：Ｓｔａｇｅ－ＩＤ、ＩＣカードのカードＩＤ：Ｓ－ＩＤ及びクレジットデータとを不正使用者に盗み見られたとしても、課金によりそのＩＣカードの最近のクレジットデータは減少しているので、クレジットデータをチェックすることで不正使用者からのアクセスであることを検出することができる。また、サーバ１側で、ゲームパスワードＧ－ＰＷを暗号化する鍵データとして、ＩＣカードのカードＩＤ：Ｓ－ＩＤ及びクレジットデータの組を使用することができる。その場合は、クレジットデータが変化するまでの間だけ有効なゲームパスワードＧ－ＰＷを利用することができる。

【００５２】第二の実施の形態例の第二の変形例として、サーバ１は、その外部記憶ファイル５に、カードＩＤ：Ｓ－１Ｄとその所有者に与えたゲームパスワードＧ－ＰＷとの対応テーブルを記録する。サーバ１は、課金処理の時に、外部記憶ファイル５にカードＩＤ：Ｓ－ＩＤと新たに与えるゲームパスワードＧ－ＰＷとを記録する。従って、一つのカードＩＤ：Ｓ－ＩＤに対して複数のゲームパスワードが記録されることもある。センタにあるサーバ１の外部ファイル５に、カードＩＤ：Ｓ－ＩＤと提供したゲームパスワードＧ－ＰＷとの対応テーブルを記録しておくことで、正規ユーザが正規のＩＣカー

ドを所有していれば、他の場所、他のゲーム機からでもサーバにアクセスしてゲームパスワードＧ－ＰＷとをダウンロードすることが可能になり、ユーザの利便性を高めることができる。

【００５３】図６は、第二の実施の形態例のフローチャート図である。このフローチャート図は、ゲーム機６とサーバ１との間のデータの送受信、それに対するそれぞれの処理内容を示す。

【００５４】最初に、ユーザは、サンプルゲームのソフトウエアを入手し、そのサンプルゲームをゲーム機６で実行する（Ｓ３０）。そして、フリーサンプル部分が終了すると、それから先を使用する為の使用許諾パスワードである、ゲームパスワードが必要になる。そこで、ゲーム機６をセンタのサーバ１に接続し（Ｓ３２）、個人認証情報と共に、ゲームＩＤ：Ｇ－ＩＤ、ステージＩＤ：Ｓｔａｇｅ－ＩＤ、ＩＣカードのカードＩＤ：Ｓ－ＩＤをサーバ１に送信する（Ｓ３４）。

【００５５】それに対して、サーバ１では、個人認証情報のユーザＩＤ：Ｙ－ＩＤとユーザパスワードＹ－ＰＷとをチェックし、認証を行う。そして、正規ユーザであることが確認され、課金処理と共に、ゲームＩＤ：Ｇ－ＩＤとステージＩＤ：Ｓｔａｇｅ－ＩＤに対応するゲームパスワードＧ－ＰＷをカードＩＤ：Ｓ－ＩＤを鍵データにして暗号化する（Ｓ３６）。そして、暗号化されたゲームパスワードＧ－ＰＷが送られる（Ｓ３８）。

【００５６】ゲーム機６では、モデム２０の不揮発性メモリ２５内に、その暗号化されたゲームパスワードＧ－ＰＷと共に、カードＩＤ：Ｓ－ＩＤを暗号化して記録する（Ｓ４０）。むろん、ゲームパスワードＧ－ＰＷに対して、そのゲームＩＤ：Ｇ－ＩＤとステージＩＤ：Ｓｔａｇｅ－ＩＤも記録される。そして、ゲーム機６はサーバ１との通信を切断する（Ｓ４２）。その後、ゲーム機６では、サーバ１との接続を行うことなく、正規のＩＣカードが挿入されて、その鍵データであるカードＩＤ：Ｓ－ＩＤが一致する場合のみ、記録されているゲームパスワードＧ－ＰＷを鍵データで復号化して、必要とするプログラムの使用を可能にする（Ｓ４４）。

【００５７】更に、ＩＣカードのみを所有したユーザが、別の場所の別のゲーム機６からサーバ１に接続して（Ｓ４６）、認証情報とゲームＩＤ：Ｇ－ＩＤ、そのステージＩＤ：Ｓｔａｇｅ－ＩＤ及びカードＩＤ：Ｓ－ＩＤをサーバに送信し（Ｓ４８）、それに対して、サーバ１は、外部記録ファイル５の参照テーブルから、一旦与えられたゲームパスワードをカードＩＤ：Ｓ－ＩＤを鍵データにして暗号化して、ゲーム機６に送信する（Ｓ５０）。この場合は、ＩＣカードを所有する正規のユーザは、必要に応じてサーバ１からゲームパスワードをダウンロードすることができる。

【００５８】図７は、更に第二の実施の形態例の変形例を示す図である。図７には、図５と同じ引用番号が付されている。上記の第二の実施の形態例では、ゲーム機６のモデム２０内の不揮発性メモリ２５に、カードＩＤ：Ｓ－ＩＤを鍵データにして暗号化されたゲームパスワードと共に、その鍵データも記録していた。それに対して、この変形例では、モデム内の不揮発性メモリ２５には、鍵データのカードＩＤ：Ｓ－ＩＤを記録せずに、その鍵データにより暗号化されたゲームパスワードＧ－ＰＷのみをゲームＩＤとステージＩＤに関連付けて記録するだけである。

【００５９】そして、ゲームパスワードを利用する時は、挿入されたＩＣカードのカードＩＤ：Ｓ－ＩＤを鍵データにして記録されたゲームパスワードＧ－ＰＷを復号化して使用する。正しいＩＣカードが挿入されなければ、正しい復号化されたパスワードが生成されないので、同様に不正利用に対する耐性を高くすることができる。しかも、モデム２０内の不揮発性メモリ２５内に鍵データを記録しないので、その鍵データが不正に複製されるリスクをなくすことができる。

【００６０】この変形例は、図４で示した個人認証情報をカードＩＤ：Ｓ－ＩＤを鍵データにして暗号化する例と共に利用される時、最も効果が大きい。

【００６１】

【発明の効果】以上説明した通り、本発明によれば、個人認証情報であるユーザＩＤとユーザパスワードとを、正規ユーザに配布されるＩＣカードのカードＩＤを鍵データとしてゲーム機内のメモリに記録する様にしたので、サーバにアクセスするたびに無意味な英数字列の入力を行う必要がなく、しかも、認証情報が記録されるゲーム機のモデムと鍵データが記録されたＩＣカードとを物理的に分離したことで、認証情報が不正に使用されることに対する耐性を高くすることができる。

【００６２】更に、本発明によれば、使用許諾パスワードをＩＣカードのカードＩＤを鍵データに利用して暗号化したデータを、使用許諾パスワードとしてユーザに提供する様にしたので、ユーザに対して使用許諾パスワードそのものを知らせずにサービスを提供することができ、使用許諾パスワードの不正コピーによる不正使用を防止することができる。また、正規ユーザが所有するＩＣカードが挿入された時に、そのカードＩＤを鍵データにして使用許諾パスワードを復号化することができるようにしたので、不正使用に対する耐性を高くすることができる。

【００６３】また、サーバ側で、ＩＣカードの最新のクレジットデータを保管しておくことで、多数の不正使用者がカードＩＤ等を送信して使用許諾パスワードの提供を求めても、最新クレジットデータを照合することで、その要求を拒絶することが可能になる。

【図面の簡単な説明】

【図１】第一の実施の形態例の全体構成を示す図である。

【図２】ゲーム機とＩＤカードの詳細構成を示す図である。

【図３】ゲーム機のモデム内の不揮発性メモリ内に情報が保存され、それが使用される場合のフローチャートを示す図である。

【図４】第一の実施の形態例の変形例を示す図である。

【図５】第二の実施の形態例の概略図である。

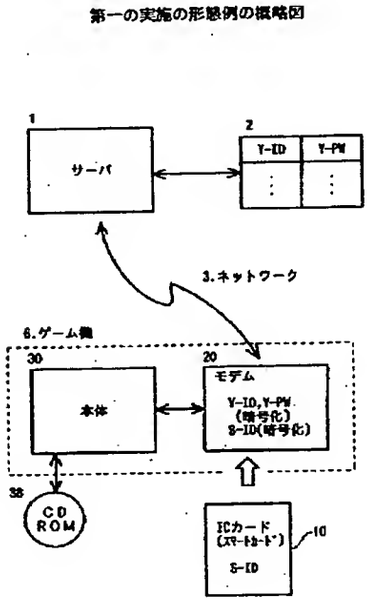
【図６】第二の実施の形態例のフローチャート図である。

【図７】第二の実施の形態例の変形例を示す図である。

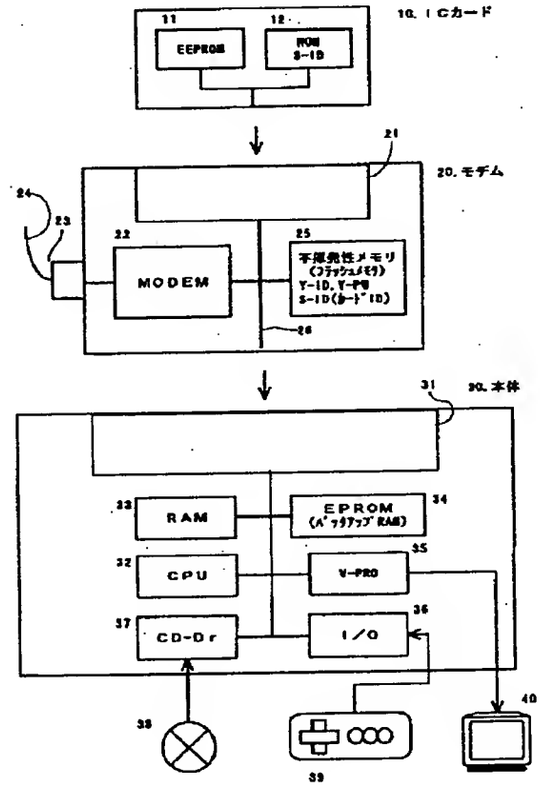
＊【符号の説明】

| | |
|---|---|
| １ | サーバ |
| ６ | ゲーム機、通信端末装置 |
| １０ | ＩＣカード |
| ２０ | モデム |
| ２５ | 不揮発性メモリ、記録媒体 |
| Ｓ－ＩＤ | カードＩＤ |
| Ｙ－ＩＤ | ユーザＩＤ |
| Ｙ－ＰＷ | ユーザパスワード |
| Ｇ－ＰＷ | ゲームパスワード、使用許諾パスワード |

【図１】

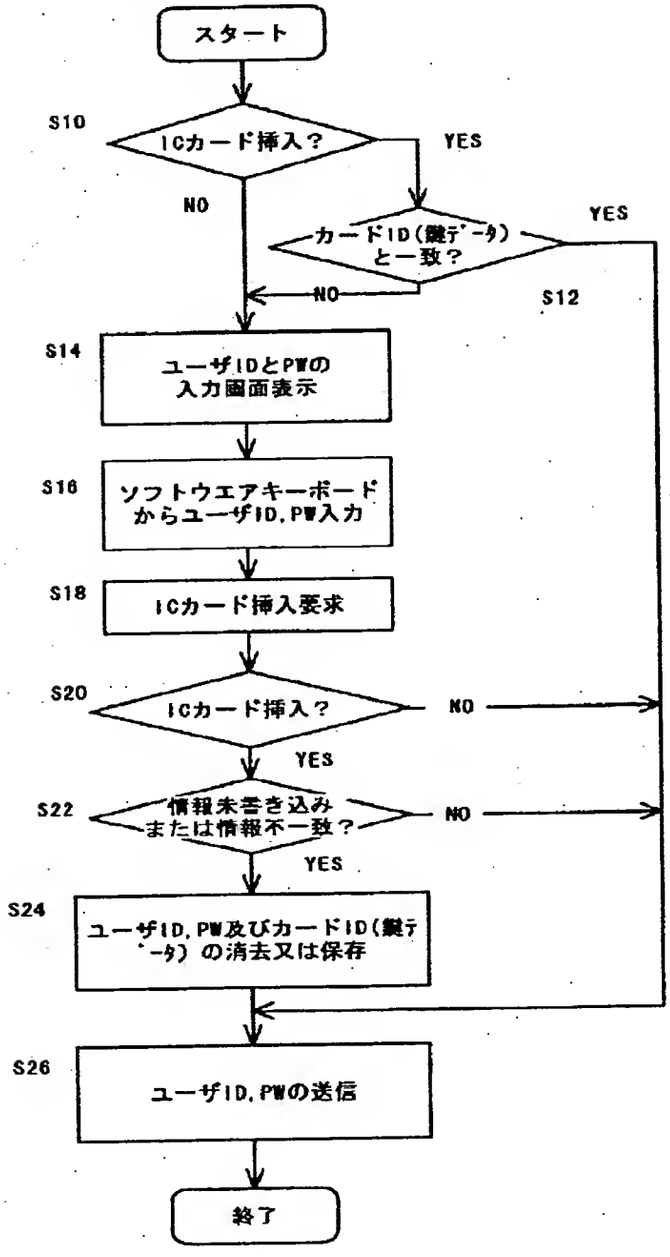



【図２】



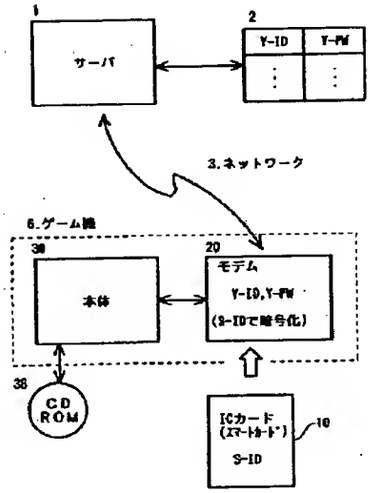
【図３】

第一の実施の形態例のフローチャート図



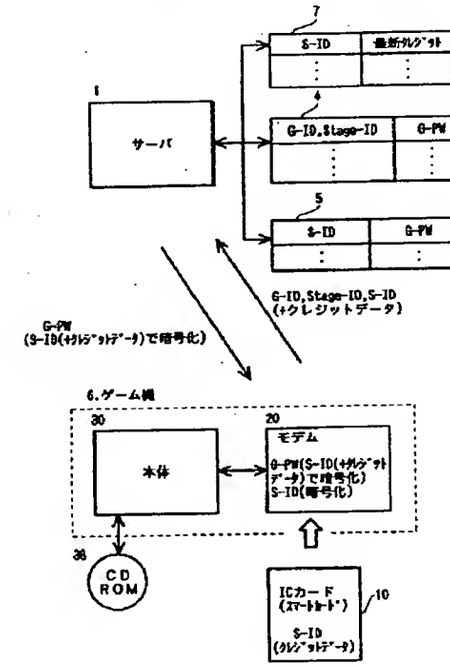

【図４】

第一の実施の形態例の変形例

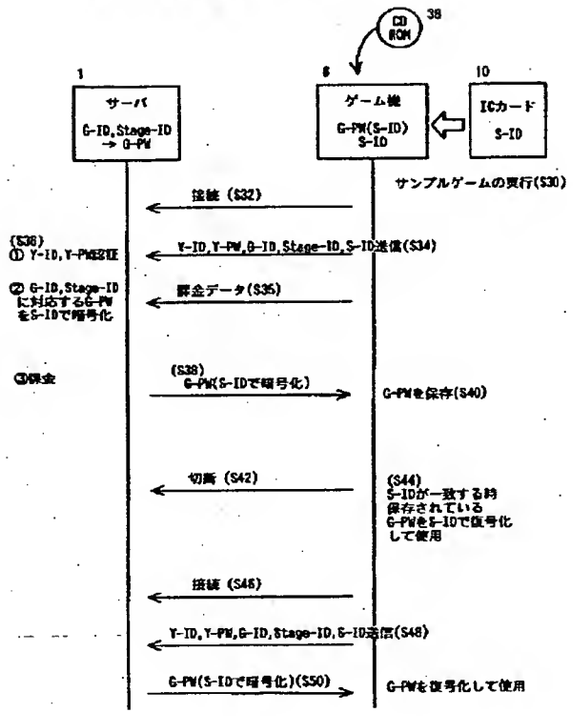



【図５】

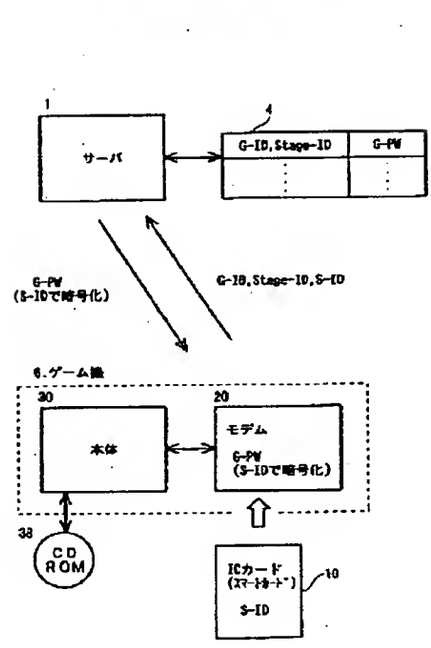
第二の実施の形態例の概略図



【図６】




【図７】




フロントページの続き

| (51)Int.Cl.[5] | 識別記号 | FI | |
|---|---|---|---|
| G07F 7/08 | | G07F 7/08 | S |